UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/594,306	09/27/2006	Paolo Milani Comparetti	09952.0074	3388

22852 7590 09/30/2010
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
09/30/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/594,306	**Applicant(s)** MILANI COMPARETTI ET AL.	
	Examiner MICHAEL J. SIMITOSKI	**Art Unit** 2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 September 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *39-77* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *39-77* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 September 2006* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *9/27/06*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. The IDS of 9/27/2006 was received and considered.

2. Claims 39-77 are pending.

Specification

3. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 57-76 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

a. Regarding claims 57-76, the claims are directed to a system including modules, which could be directed to software, per se. The software embodiment does not fall within one of the statutory classes of invention defined under 35 U.S.C. §101.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this

> subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 39-43, 56-62 and 75-77 rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 7,716,742 to Roesch et al. (**Roesch**).

Regarding claims 39, 57 and 76-77, Roesch discloses a method of providing intrusion detection in a network wherein data flows are exchanged using associated network ports and application layer protocols, comprising the steps of: monitoring data flows in said network (monitoring traffic, col. 14, lines 50-54); detecting information on said application layer protocols involved in said monitored data flows (detect operating systems, services, col. 15, lines 1-20); and providing intrusion detection on said monitored data flows based on application layer protocols detected (detect packet characteristics indicative of operating system, services, etc., col. 12, lines 28-51).

Regarding claims 40 and 58, Roesch discloses wherein said intrusion detection is provided independently of any predefined association between said network ports and said application layer protocols (based on packet fingerprints, col. 12, lines 28-51).

Regarding claims 41 and 59, Roesch discloses wherein said step of detecting information on application layer protocols comprises passive observation of network traffic (packet detector, col. 9, lines 51-53).

Regarding claims 42 and 61, Roesch discloses wherein said step of detecting information on application layer protocols comprises using signature-matching techniques (matching fingerprints, col. 12, lines 28-51).

Regarding claims 43 and 62, Roesch discloses wherein said step of detecting information on application layer protocols in said data flows comprises the step of identifying at least one protocol in a given data flow (identify services, such as client/server, col. 15, lines 1-20).

Regarding claims 56 and 75, Roesch discloses wherein said step of providing intrusion detection based on said information on application layer protocols comprises the steps of: establishing a network policy (intrusion detection policy, col. 15, lines 21-30), and generating a security event whenever a protocol is detected in violation of said network policy (generate alarm/report when an attack is found, col. 15, lines 21-30).

Regarding claim 60, Roesch discloses module is a sniffer (Fig. 9).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 44 and 63 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Roesch**, as applied to claims 39 and 57 above, in view of U.S. Patent 7,305,708 to Norton et al. (**Norton**).

Regarding claims 44 and 63, Roesch discloses wherein said step of providing intrusion detection comprises detection of misuse by matching at least one of a given data packet and data flow regardless of the service ports involved, based on said information on application layer protocols (input to intrusion detection systems, col. 15, lines 21-30), but lacks explicitly signature-based intrusion detection. However, Norton teaches detecting a particular application-layer protocol in network traffic (HTTP, col. 15, line 33 – col. 16, line 41) and matching the packet against signatures (col. 18, lines 1-35) to narrow the search required of a detection engine (col. 15, lines 33-43). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Roesch to include a signature-based intrusion detection. One of ordinary skill in the art would have been motivated to perform such a modification to monitor a session for intrusions, as taught by Norton.

10. Claims 45-47, 50-53, 64-66 and 69-72 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Roesch**, as applied to claims 39 and 57 above, in view of "Intrusion detection system for high-speed network" by Yang et al. (**Yang**).

Regarding claims 45 and 64, Roesch lacks providing intrusion detection based on a plurality of predefined sets of analysis tasks and misuse signatures for a plurality of said protocols, and comprises selecting out of said plurality a set related to at least one protocol in a given data flow and at least one of the steps of: performing over said data flow the selected set of analysis tasks; and performing signature matching over said data flow against the selected set of misuse signatures. However, Yang teaches providing intrusion detection based on a plurality of predefined sets of analysis tasks (packet capture, filter and protocol analysis, Fig. 1, p. 1290, §3.3) and misuse signatures for a plurality of said protocols (Fig. 1, rule-based detection), and comprises selecting out of said plurality a set related to at least one protocol in a given data flow (determining application protocol, p. 1290, §3.3) and at least one of the steps of: performing over said data flow the selected set of analysis tasks (invoking decoding modules, p. 1290, §3.3); and performing signature matching over said data flow against the selected set of misuse signatures (rule-based detection, Fig. 1), to gain the benefit of efficiency (p. 1290, §3.3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Roesch to include the steps describe above. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of efficiency, as taught by Yang.

Regarding claims 46 and 65, Roesch discloses wherein said steps of detecting information on application layer protocols and providing intrusion detection are performed within the same functional module and employing the same functional blocks of packet capture and preprocessing (Fig. 9), but lacks explicitly signature matching. However, Yang teaches a system where signature matching is used to detect intrusions in traffic that has been classified into protocols (p. 1289, Fig. 1) to gain the benefit of efficiency (p. 1290, §3.3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Roesch to include signature matching. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of efficiency, as taught by Yang.

Regarding claims 47 and 66, Roesch lacks wherein said signature-matching is performed by comparing monitored traffic with a set of protocol detection signatures having the following characteristics: the set of signatures is specified in a language similar to the signature language used to specify misuse signatures in said network intrusion detection system, and each said signature specifies a respective protocol that is detected if the signature is triggered. However, Yang teaches a system wherein signature-matching is performed by comparing monitored traffic with a set of protocol detection signatures (signatures based on the RCE standard, p. 1292, §3.4.1) having the following characteristics: the set of signatures is specified in a language similar to the signature language used to specify misuse signatures in said network intrusion detection system (rule description language, p. 1292, §3.4.1), and each said signature specifies a respective protocol that is detected if the signature is triggered (APPWatch identifies application protocols of packets, which is then used to detect anomalous packets based on the RFC, p. 1290, §3.3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Roesch such that said signature-matching is performed by comparing monitored traffic with a set of protocol detection signatures having the following characteristics: the set of signatures is specified in a language similar to the signature language used to specify misuse signatures in said network intrusion detection system, and each said signature specifies a respective protocol that is detected if the signature is triggered. One of ordinary skill in the art would have been motivated to perform such a modification to identify an application protocol and monitor for intrusion based on the protocol to gain efficiency, as taught by Yang.

Regarding claims 50 and 69, Roesch, as modified, teaches leaving out signatures exclusively matching a pattern in client behavior (determining if the traffic is from a client or server, col. 15, lines 1-

9). As modified, it would have been obvious to use the signatures of Yang to eliminate the client behavior in accordance with the separation of client and server traffic by Roesch, for the reasons above.

Regarding claims 51 and 70, Roesch teaches characterizing a network (i.e. classifying data flows related to each server application in said network , col. 14, lines 42-44), but lacks wherein detecting information on application layer protocols involved in said data flows comprises the characterizing and classifying. However, for the reasons stated above, it would have been obvious to utilize Yang's classification of application protocol to characterize each server application on the network.

Regarding claims 52 and 71, Roesch discloses wherein said step of characterizing and classifying data flows comprises monitoring features from the group of: packet size, packet arrival times, TCP flags and header information (col. 14, lines 54-55).

Regarding claims 53 and 72, Roesch discloses wherein said step of characterizing and classifying data flows comprises classifying data flows and services into a number of flow classes (col. 15, lines 1-9).

11. Claims 48-49 and 67-68 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Roesch** and **Yang**, as applied to claims 47 and 66 above, in view of U.S. Patent 7,620,988 to **Hernacki**.

Regarding claims 48 and 67, Roesch, as modified, lacks wherein each said signature is designed to attempt to match a pattern that is unique to a given protocol and at the same time is frequently used in said protocol. However, Hernacki teaches determining an application protocol in network traffic by explicitly comparing packet payload content to patterns for a match (col. 3, lines33-36). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Roesch, as modified, such that each said signature is designed to attempt to match a pattern that is unique to a given protocol and at the same time is frequently used in said protocol. One of ordinary skill in the art would have been motivated to perform such a modification to identify the application using patterns, as taught by Hernacki.

Regarding claims 49 and 68, Roesch, as modified, lacks using at least one of the signatures identifying behavior frequently present in server responses and signatures identifying common client request-server reply behavior. However, Hernacki teaches using at least one of the signatures identifying behavior frequently present in server responses and signatures identifying common client request-server reply behavior (col. 4, lines 1-5 and col. 5, lines 15-27). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Roesch to include using at least one of the signatures identifying behavior frequently present in server responses and signatures identifying common client request-server reply behavior. One of ordinary skill in the art would have been motivated to perform such a modification to identify the application using patterns, as taught by Hernacki.

12. Claims 54-55 and 73 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Roesch** and **Yang**, as applied to claims 51, 70 and 39 above, in view of U.S. Patent 7,660,248 to Duffield et al. **(Duffield**).

Regarding claims 54 and 73, Roesch lacks wherein said step of characterizing and classifying data flows comprises at least one of discriminating between interactive and non-interactive traffic and identifying specific protocols. However, Duffield teaches that classification of packet flows is useful to determine different treatments to those packets and flows (col. 2, lines 43-46, lines 56-59, col. 10, lines 45-48) including categories of interactive and bulk (col. 5, lines 46-56). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Roesch to classify data flows by discriminating between interactive and non-interactive traffic and identifying specific protocols. One of ordinary skill in the art would have been motivated to perform such a modification to treat the traffic differently, as taught by Duffield.

Regarding claim 55, Roesch lacks wherein said step of detecting information on application layer protocols in said data flows comprises producing a map of associations between application layer protocols and network ports present in said network, and said step of providing intrusion detection is performed on said associated network ports. However, Duffield teaches producing a map of associations between application layer protocols and network ports present in said network (mapping class of traffic found on a port to the port itself, 45-50), and said step of providing intrusion detection is performed on said associated network ports (applying QoS treatment to the traffic, col. 10, lines 53-56). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Roesch, as modified above, to include producing a map of associations between application layer protocols and network ports present in said network (using the signatures), and said step of providing intrusion detection is performed on said associated network ports (based on the aggregate result). One of ordinary skill in the art would have been motivated to perform such a modification to reduce the need for full-time payload analysis, as taught by Duffield.

13. Claim 74 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Roesch**, as applied to claim 58 above, in view of **Duffield**.

Regarding claim 74, Roesch lacks wherein said step of detecting information on application layer protocols in said data flows comprises producing a map of associations between application layer protocols and network ports present in said network, and said step of providing intrusion detection is performed on said associated network ports. However, Duffield teaches producing a map of associations between application layer protocols and network ports present in said network (mapping class of traffic found on a port to the port itself, 45-50), and said step of providing intrusion detection is performed on said associated network ports (applying QoS treatment to the traffic, col. 10, lines 53-56). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Roesch, as modified above, to include producing a map of associations between application layer protocols and network ports present in said network (using the signatures), and said step of providing intrusion detection is performed on said associated network ports (based on the aggregate result). One of ordinary skill in the art would have been motivated to perform such a modification to reduce the need for full-time payload analysis, as taught by Duffield.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL J. SIMITOSKI whose telephone number is (571)272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571)272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

September 27, 2010
/Michael J Simitoski/
Primary Examiner, Art Unit 2439